

# Generalized Doubly Stochastic and Permutation Matrices Over a Ring

Peter M. Gibson

*University of Alabama in Huntsville*  
*Huntsville, Alabama 35807*

Submitted by Hans Schneider

---

## ABSTRACT

Let  $R$  be a ring with unity. A combinatorial argument is used to show that the  $R$ -module  $\Delta_n(R)$  of all  $n \times n$  matrices over  $R$  with constant row and column sums has a basis consisting of permutation matrices. This is used to characterize orthogonal matrices which are linear combinations of permutation matrices. It is shown that all bases of  $\Delta_n(R)$  consisting of permutation matrices have the same cardinality, and other properties of bases of  $\Delta_n(R)$  are investigated.

---

## 1. INTRODUCTION

Throughout this paper  $R$  is a ring with unity  $e$ ,  $e \neq 0$ . Let  $x \in R$ . If  $A$  is an  $n \times n$  matrix over  $R$  such that each row and column sum of  $A$  is equal to  $x$ , then  $A$  is said to be a *generalized doubly stochastic* (g.d.s.) *matrix corresponding to  $x$* . If  $K = (k_{ij})$  is an  $m \times n$  matrix over the integers  $Z$ , then  $Kx = (a_{ij})$  is the  $m \times n$  matrix over  $R$  with  $a_{ij} = k_{ij}x$  for  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ . If  $P$  is a permutation matrix over  $Z$ , then  $Pe$  is called a *permutation matrix over  $R$* . Let  $\Delta_n(R)$  denote the set of all  $n \times n$  g.d.s. matrices over  $R$ . It is easy to see that  $\Delta_n(R)$  is a submodule of the (left)  $R$ -module of all  $n \times n$  matrices over  $R$ , and that every  $n \times n$  permutation matrix over  $R$  is in  $\Delta_n(R)$ .

In this paper a combinatorial argument is used to prove that  $\Delta_n(R)$  has a basis consisting of  $d_n = n^2 - 2n + 2$  permutation matrices. Applying this result, the question considered by J. Kapoor [3] of which real orthogonal matrices can be expressed as linear combinations of permutation matrices is answered by showing that such real orthogonal matrices are those which are g.d.s. matrices corresponding to  $\pm 1$ . For some rings  $\Delta_n(R)$  has bases with more than  $d_n$  elements. However, it is shown that every basis of  $\Delta_n(R)$  consisting of permutation matrices has cardinality  $d_n$ . We conclude by considering certain sets of permutation matrices that are bases of  $\Delta_n(Z)$ .

## 2. A BASIS OF PERMUTATION MATRICES

**THEOREM 2.1.** *The  $R$ -module  $\Delta_n(R)$  has a basis consisting of  $d_n = n^2 - 2n + 2$  permutation matrices.*

*Proof.* Let  $I$  be the  $n \times n$  identity matrix and  $Q = (q_{ij})$  the  $n \times n$  permutation matrix over  $Z$  with  $q_{i,i+1} = 1$  for  $i = 1, \dots, n$  (modulo  $n$ ). Let  $M = (m_{ij}) = I + Q$ , and suppose that the  $s = n^2 - 2n$  zero entries of  $M$  are  $m_{i_1 j_1}, \dots, m_{i_s j_s}$ . For each  $k = 1, \dots, s$ , there is a unique  $n \times n$  permutation matrix  $P_k = (p_{ij})$  over  $Z$  such that  $p_{k k} = 1$  and  $p_{ij} \leq m_{ij}$  whenever  $(i, j) \neq (i_k, j_k)$  (see for example [1]). Let  $P_{s+1} = Q$  and  $P_{s+2} = I$ . Suppose that  $x_1, \dots, x_{s+2} \in R$  with  $\sum_{k=1}^{s+2} x_k P_k e = 0$ . For  $k = 1, \dots, s$ , the  $(i_k, j_k)$  entry of  $P_k e$  is  $e$ , while the  $(i_k, j_k)$  entry of  $P_m e$  is zero whenever  $m \neq k$ . Hence,  $x_k = 0$  for  $k = 1, \dots, s$ . It now follows that  $x_{s+1} = x_{s+2} = 0$ . Therefore the set  $\Gamma = \{P_k e : k = 1, \dots, s+2\}$  of permutation matrices over  $R$  is linearly independent. For  $A = (a_{ij}) \in \Delta_n(R)$ , let

$$B = (b_{ij}) = A - \sum_{k=1}^s a_{k i_k} P_k e,$$

$$C = (c_{ij}) = B - b_{n1} P_{s+1} e - b_{nn} P_{s+2} e.$$

Clearly  $C \in \Delta_n(R)$  and all entries of  $C$  are zero except possibly  $c_{ii}$  and  $c_{i,i+1}$  for  $i = 1, \dots, n-1$ . It is easy to see that this implies that  $C = 0$ . Therefore  $\Gamma$  spans  $\Delta_n(R)$ , and thus  $\Gamma$  is a basis of  $\Delta_n(R)$  with cardinality  $d_n$ . ■

**REMARK.** Theorem 2.1 implies that an  $n \times n$  matrix  $A$  over  $R$  can be expressed as a linear combination of permutation matrices if and only if  $A \in \Delta_n(R)$ . An analogous result holds for matrices over arbitrary rings. Let  $A$  be a matrix over a ring  $K$ . It follows from the proof of Theorem 2.1 that  $A$  can be expressed as  $A = \sum_{k=1}^{d_n} P_k x_k$  for some permutation matrices  $P_1, \dots, P_{d_n}$  over  $Z$  and  $x_1, \dots, x_{d_n} \in K$  if and only if there exists  $x \in K$  such that each row and column sum of  $A$  is equal to  $x$ .

## 3. ORTHOGONAL MATRICES

Let  $A$  be an  $n \times n$  matrix over  $R$ , and let  $A^T$  be the transpose of  $A$ . If  $AA^T$  is the  $n \times n$  identity matrix over  $R$ , then  $A$  is said to be an orthogonal matrix.

**THEOREM 3.1.** *If  $A$  is an orthogonal matrix over  $R$ , then the following are equivalent:*

- (a)  *$A$  is a linear combination of permutation matrices,*
- (b)  *$A \in \Delta_n(R)$ ,*
- (c)  *$A$  is a g.d.s. matrix corresponding to some  $x$  in  $R$  with  $x^2 = e$ .*

*Proof.* It is immediate that (a) implies (b), and it follows from Theorem 2.1 that (c) implies (a). Suppose that (b) holds. Let  $x \in R$  such that  $A$  corresponds to  $x$ . Since  $A = (a_{ij})$  is an orthogonal matrix,

$$\sum_{k=1}^n a_{ik} a_{jk} = \delta_{ij} e, \quad i, j = 1, \dots, n,$$

where  $\delta_{ij}$  is the Kronecker delta. Therefore,

$$e = \sum_{j=1}^n \delta_{ij} e = \sum_{j=1}^n \sum_{k=1}^n a_{ik} a_{jk} = \sum_{k=1}^n a_{ik} x = x^2.$$

Hence, (b) implies (c). ■

J. Kapoor [3] considered the question of which real orthogonal matrices can be expressed as linear combinations of permutation matrices. By using a rather involved argument he showed that if a real orthogonal matrix is a linear combination of permutation matrices, then the sum of the coefficients in this linear combination must be  $\pm 1$ . An answer to Kapoor's question immediately follows from Theorem 3.1 for orthogonal matrices over any field.

**COROLLARY 3.2.** *An  $n \times n$  orthogonal matrix over a field can be expressed as a linear combination of permutation matrices if and only if  $A$  is a g.d.s. matrix corresponding to  $\pm 1$ .*

Analogous questions could be answered for other special matrices by using Theorem 2.1. For example it is easy to obtain the following.

**THEOREM 3.3.** *An  $n \times n$  unitary matrix  $A$  over the complex field can be expressed as a linear combination of permutation matrices if and only if  $A$  is a g.d.s. matrix corresponding to  $x$  for some complex number  $x$  of modulus 1.*

## 4. CARDINALITY OF BASES

It follows from Theorem 2.1 that if  $R$  is commutative, then every basis  $\Gamma$  of  $\Delta_n(R)$  has cardinality  $|\Gamma| = d_n$ . However this does not hold in general. To see this, let  $R_0$  be the ring of all linear operators on the real vector space  $V$  of all polynomials in  $x$  with real coefficients, and let  $s$  be any integer with  $s \geq d_n$ . According to Theorem 2.1 there exist  $n \times n$  permutation matrices  $P_1, \dots, P_{d_n}$  over  $Z$  such that  $\Gamma = \{P_k e : k = 1, \dots, d_n\}$  is a basis of  $\Delta_n(R_0)$ . Let  $t = s - d_n + 1$ . For  $k = 1, \dots, t$ , let  $\sigma_k(\sum_i a_i x^i) = \sum_i a_{i+k-1} x^i$  for all  $\sum_i a_i x^i \in V$ . It is not difficult to show that  $\{\sigma_1, \dots, \sigma_t\}$  is a basis of  $R_0$  considered as an  $R_0$ -module (see for example [2, p. 190]). Hence, it follows that the set  $\Gamma'$  obtained from  $\Gamma$  by replacing  $P_1 e$  with  $P_1 \sigma_1, \dots, P_1 \sigma_t$  is a basis of  $\Delta_n(R_0)$  with  $|\Gamma'| = s$ . Therefore there exists a basis of  $\Delta_n(R_0)$  with cardinality  $s$  for every integer  $s \geq d_n$ . We shall see that if  $\Gamma$  is any basis of  $\Delta_n(R)$  consisting of permutation matrices, then  $|\Gamma| = d_n$ .

If  $A$  is an  $n \times n$  matrix over  $R$ , let  $A^*$  denote the  $n^2 \times 1$  matrix over  $R$  whose entries are those of  $A$  in lexicographic order. If  $\Gamma = \{A_1, \dots, A_k\}$  is a set of  $n \times n$  matrices over  $R$ , let  $\Gamma^*$  denote the  $n^2 \times k$  matrix whose columns are  $A_1^*, \dots, A_k^*$ .

**THEOREM 4.1.** *If  $\Gamma$  is a basis of  $\Delta_n(R)$  consisting of permutation matrices, then  $|\Gamma| = d_n$ .*

*Proof.* Suppose that  $\Gamma$  is a basis of  $\Delta_n(R)$  consisting of permutation matrices, and let  $\Gamma_0$  be the set of permutation matrices over  $Z$  such that  $\Gamma = \{P e : P \in \Gamma_0\}$ . Assume there exist nonzero  $c_1, \dots, c_k \in Z$  and distinct  $P_1, \dots, P_k \in \Gamma_0$  such that  $\sum_{i=1}^k c_i P_i = 0$ . We may assume that  $c_1, \dots, c_k$  are relatively prime. It then follows that

$$\sum_{i=1}^k c_i e P_i e = \left( \sum_{i=1}^k c_i P_i \right) e = 0,$$

where  $c_i e \neq 0$  for some  $1 \leq i \leq k$ , and we see that  $\Gamma$  is linearly dependent. Therefore  $\Gamma_0$  must be linearly independent. It now follows from Theorem 2.1 that  $|\Gamma| = |\Gamma_0| = m \leq d_n$ . Suppose that  $m < d_n$ . Let  $A = \Gamma_0^*$ , and let  $B$  be the  $n^2 \times (n! - m)$  matrix whose columns are the matrices  $P^*$  for the  $n \times n$  permutation matrices  $P$  over  $Z$  for which  $P \notin \Gamma_0$ . Since  $\Gamma_0$  is linearly independent, there exists an  $n^2 \times n^2$  matrix  $Q$  over  $Z$  such that  $\det Q = \pm 1$

and

$$QA = \begin{bmatrix} A_1 \\ 0 \end{bmatrix}, \quad QB = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix},$$

where  $A_1$  is an  $m \times m$  matrix and  $B_1$  is an  $m \times (n! - m)$  matrix. Since  $\Gamma$  spans  $\Delta_n(R)$ , there exists a matrix  $X$  over  $R$  such that  $AeX = Be$ . It follows that

$$\begin{bmatrix} A_1 \\ 0 \end{bmatrix} eX = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} e.$$

Hence  $B_2e = 0$ . However, since  $m < d_n = \dim \Delta_n(Z)$ , we see that  $B_2 \neq 0$ . Therefore  $R$  has as characteristic some integer  $k \geq 2$  that divides each entry of  $B_2$ . Let  $p$  be a positive prime such that  $p$  divides  $k$ . Then  $B_2 = 0$  over the field  $Z_p$  of integers modulo  $p$ . Hence it follows that  $\Delta_n(Z_p)$  is spanned by a set of  $m$  permutation matrices. This contradicts  $\dim \Delta_n(Z_p) = d_n$ . Therefore  $|\Gamma| = d_n$ . ■

## 5. BASES OF $\Delta_n(Z)$

We say that a set  $\Gamma$  of  $n \times n$  permutation matrices over  $Z$  is a *combinatorial basis* of  $\Delta_n(Z)$  if there exist  $n \times n$  permutation matrices  $U$  and  $V$  over  $Z$  such that  $\{UPV : P \in \Gamma\}$  is the set of  $d_n$   $n \times n$  permutation matrices over  $Z$  used in the proof of Theorem 2.1. Combinatorial bases  $\Gamma$  of  $\Delta_n(Z)$  can be characterized in terms of the  $n^2 \times d_n$  matrix  $\Gamma^*$ .

**THEOREM 5.1.** *Let  $\Gamma$  be a set of  $d_n$   $n \times n$  permutation matrices over  $Z$ . Then  $\Gamma$  is a combinatorial basis of  $\Delta_n(Z)$  if and only if  $\Gamma^*$  has a  $(d_n - 2) \times d_n$  submatrix with precisely one 1 in each row and no more than one 1 in each column.*

*Proof.* It is easy to see that every set  $\Gamma$  of five  $3 \times 3$  permutation matrices over  $Z$  is a combinatorial basis of  $\Delta_3(Z)$  and also has the property that there exists a  $3 \times 5$  submatrix of  $\Gamma^*$  with precisely one 1 in each row and no more than one 1 in each column. Hence we may assume that  $n \geq 4$ . Suppose that  $\Gamma^*$  has a  $(d_n - 2) \times d_n$  submatrix  $C$  with precisely one 1 in each row and no more than one 1 in each column. Let  $A = (a_{ij})$  be the  $(0, 1)$ -matrix for which each entry of  $A^*$  is 0 or 1 according as it does or does not

correspond to a row of  $\Gamma^*$  in  $C$ . Assume that  $A$  is not fully indecomposable. Since  $C$  has zero columns, there are  $n \times n$  permutation matrices  $P = (p_{ij})$  such that  $p_{ij} \leq a_{ij}$  for  $i, j = 1, \dots, n$ . Hence there exist  $n \times r$  permutation matrices  $U$  and  $V$  such that

$$UAV = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ X_{21} & A_2 & \cdots & 0 \\ \vdots & & & \vdots \\ X_{k1} & X_{k2} & \cdots & A_k \end{bmatrix},$$

where  $k > 1$  and  $A_1, \dots, A_k$  are nonzero matrices of order 1 or fully indecomposable  $(0, 1)$ -matrices of order greater than 1. Since each row of  $C$  contains precisely one 1 and no column of  $C$  contains more than one 1, for each entry  $a_{rs} = 0$  of  $A$  there is  $P = (p_{ij}) \in \Gamma$  such that  $p_{rs} = 1$  and  $p_{ij} \leq a_{ij}$  whenever  $(i, j) \neq (r, s)$ . Therefore each entry of  $X_{ij}$  equals 1 for  $i = 2, \dots, k$ ,  $j = 1, \dots, k-1$ . Hence, since  $n \geq 4$ , it follows that  $A$  has more than  $2n$  entries equal to 1. This contradicts  $A$  having  $n^2 - (d_n - 2) = 2n$  entries equal to 1. Therefore  $A$  is a fully indecomposable  $n \times n$   $(0, 1)$ -matrix with  $2n$  entries equal to 1. Hence there exist  $n \times r$  permutation matrices  $U$  and  $V$  such that  $UAV = M$ , where  $M$  is the matrix  $M = I + Q$  in the proof of Theorem 2.1. Since  $C$  has two zero columns, there exist distinct  $P = (p_{ij})$  and  $P' = (p'_{ij})$  in  $\Gamma$  such that  $p_{ij} \leq a_{ij}$  and  $p'_{ij} \leq a_{ij}$  for  $i, j = 1, \dots, n$ . It follows that  $\{UPV, UP'V\} = \{I, Q\}$ . Moreover, for each additional  $P'' = (p''_{ij}) \in \Gamma$  there exists an entry  $a_{rs} = 0$  of  $A$  such that  $p''_{rs} = 1$  and  $p''_{ij} \leq a_{ij}$  whenever  $(i, j) \neq (r, s)$ . Hence we see that  $\{UPV : P \in \Gamma\}$  is the set of  $d_n$   $n \times n$  permutation matrices over  $Z$  used in the proof of Theorem 2.1, and thus  $\Gamma$  is a combinatorial basis of  $\Delta_n(Z)$ . The converse readily follows. ■

Combinatorial bases  $\Gamma$  of  $\Delta_n(Z)$  are easily found, and have the property that  $\{Pe : P \in \Gamma\}$  is a basis of  $\Delta_n(R)$  for every  $R$ . Indeed, every basis of  $\Delta_n(Z)$  has this property.

**THEOREM 5.2.** *Let  $\Gamma$  be a set of  $n \times n$  permutation matrices over  $Z$ . Then  $\{Pe : P \in \Gamma\}$  has a basis of  $\Delta_n(R)$  for every  $R$  if and only if  $\Gamma$  is a basis of  $\Delta_n(Z)$ .*

*Proof.* Suppose that  $\Gamma = \{P_1, \dots, P_{d_n}\}$  is a basis of  $\Delta_n(Z)$ . Let  $\Phi = \{Q_1, \dots, Q_{d_n}\}$  be a combinatorial basis of  $\Delta_n(Z)$ . Let  $A \in \Delta_n(R)$ . Since  $\Phi' = \{Q_k e : k = 1, \dots, d_n\}$  is a basis of  $\Delta_n(R)$ , there exist  $x_1, \dots, x_{d_n} \in R$  such that  $A = \sum_{k=1}^{d_n} x_k Q_k e$ . Since  $\Gamma$  is a basis of  $\Delta_n(Z)$ , there exist  $u_{ij} \in Z$  such that

$Q_k = \sum_{j=1}^{d_n} u_{kj} P_j$  for  $k=1, \dots, d_n$ . Then

$$A = \sum_{k=1}^{d_n} x_k \sum_{j=1}^{d_n} u_{kj} P_j e = \sum_{j=1}^{d_n} \sum_{k=1}^{d_n} x_k u_{kj} e P_j e.$$

Hence  $\Gamma' = \{P_k e : k=1, \dots, d_n\}$  spans  $\Delta_n(R)$ . Suppose that  $c_1, \dots, c_{d_n} \in R$  such that  $\sum_{k=1}^{d_n} c_k P_k e = 0$ . Since  $\Phi$  is a basis of  $\Delta_n(Z)$ , there exist  $v_{ij} \in Z$  such that  $P_k = \sum_{j=1}^{d_n} v_{kj} Q_j$  for  $k=1, \dots, d_n$ . Then

$$\sum_{j=1}^{d_n} \sum_{k=1}^{d_n} c_k v_{kj} e Q_j e = \sum_{k=1}^{d_n} c_k \sum_{j=1}^{d_n} v_{kj} Q_j e = 0.$$

Therefore, since  $\Phi'$  is a basis of  $\Delta_n(R)$ ,  $\sum_{k=1}^{d_n} c_k v_{kj} e = 0$  for  $j=1, \dots, d_n$ . Hence,  $\sum_{j=1}^{d_n} \sum_{k=1}^{d_n} c_k v_{kj} e u_{ji} e = 0$  for  $i=1, \dots, d_n$ . However, since  $\Gamma$  is linearly independent and

$$\sum_{j=1}^{d_n} \sum_{i=1}^{d_n} v_{kj} u_{ji} P_i = \sum_{j=1}^{d_n} v_{kj} \sum_{i=1}^{d_n} u_{ji} P_i = \sum_{j=1}^{d_n} v_{kj} Q_j = P_k,$$

we have  $\sum_{j=1}^{d_n} v_{kj} u_{ji} = \delta_{ki}$  for  $k, i=1, \dots, d_n$ . Hence,

$$c_i = \sum_{k=1}^{d_n} c_k \delta_{ki} e = \sum_{k=1}^{d_n} c_k \sum_{j=1}^{d_n} v_{kj} u_{ji} e = 0$$

for  $i=1, \dots, d_n$ . Therefore  $\Gamma'$  is linearly independent. Hence, if  $\Gamma$  is a basis of  $\Delta_n(Z)$ , then  $\{P e : P \in \Gamma\}$  is a basis of  $\Delta_n(R)$  for every  $R$ . The converse is trivial. ■

## REFERENCES

- 1 R. A. Brualdi and P. M. Gibson, Convex polyhedra of doubly stochastic matrices. I. Applications of the permanent function, *J. Combinatorial Theory* 22(A):194-230 (1977).
- 2 T. W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974.
- 3 J. Kapoor, Orthogonal matrices as linear combinations of permutation matrices, *Linear Algebra and Appl.* 12:189-196 (1975).

Received 13 August 1978; revised 24 April 1979